Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 39, N° 1, 2021, pág. 57–78

Imágenes de Gray de códigos consta-cíclicos sobre anillos de Galois $\mathcal{R}$ de índice de nilpotencia 3

Angel R. García-Ramírez [a] ✉, Carlos A. López-Andrade[b]
David Villa-Hernández[c]

Facultad de Ciencias Físico Matemáticas, BUAP, Avenida San Claudo y 18 Sur,
Colonia San Manuel, Puebla, Pue., México C.P. 72570.

Resumen. Estableceremos condiciones necesarias y suficientes para que la imagen bajo la función de Gray de un $\mathcal{R}$-código consta-cíclico sea un $\mathbb{F}_{p^m}$-código cuasi-cíclico. Estudiamos el anillo de vectores de Witt para obtener una manera de operar las μ-reducciones de las componentes p-ádicas de los elementos de los anillos de Galois de índice de nilpotencia 3, $\mathcal{R} = GR(p^3, m)$. Analizamos a los anillos de Galois, sus propiedades más relevantes, y en particular la representación p-ádica de sus elementos. Más adelante, examinamos la construcción del anillo de vectores de Witt y sus operaciones, en particular, obtenemos expresiones explícitas para las operaciones de suma y producto de los elementos en el anillo truncado de vectores de Witt de longitud 3, $W_3(\mathbb{F}_{p^m})$. Finalmente, utilizamos las operaciones de éstos últimos y un isomorfismo entre $GR(p^3, m)$ y $W_3(\mathbb{F}_{p^m})$ para operar las μ-reducciones antes descritas.

Palabras clave: Anillo de vectores de Witt, anillos de Galois, representación p-ádica, códigos consta-cíclicos, códigos cuasi-cíclicos.
MSC2010: 13F35, 16P10, 12F10, 94B60

Gray images of constacyclic codes over Galois rings $\mathcal{R}$ of nilpotency index 3

Abstract. We will state necessary and sufficient conditions for the image under the Gray map of a $\mathcal{R}$-constacyclic code to be $\mathbb{F}_{p^m}$-quasi-cyclic code. We study the Witt vectors to get a way to operate the μ-reduction of p-adic components of the elements of the Galois rings of nilpotency index 3,

E-mail: argr040890@gmail.com [a] ✉, clopez@fcfm.buap.mx [b], dvilla@fcfm.buap.mx [c].
Recibido: 31 March 2020, Aceptado: 1 October 2020.
Para citar este artículo: A. R. García-Ramírez, C. A. López-Andrade and David Villa-Hernández, Imágenes de Gray de códigos consta-cíclicos sobre anillos de Galois $\mathcal{R}$ de índice de nilpotencia 3, *Rev. Integr. temas mat.* 39 (2021), No. 1, 57-78. doi: 10.18273/revint.v39n1-2021005

$\mathcal{R} = GR(p^3, m)$. We analyze Galois rings, its mostly relevant properties, and we focus in the p-adic representation of their elements. Later on, we examine construction of the Witt vectors rings and its operations, in particular, we get explicit expressions for operations of addition and product of the elements in the truncated Witt vectors ring of length 3, $W_3(\mathbb{F}_{p^m})$. Finally, we will use these operations and an isomorphism between $GR(p^3, m)$ and $W_3(\mathbb{F}_{p^m})$ to get a way to operate the μ-reductions described above.

Keywords: Witt's vectors ring, Galois rings, p-adic representation, consta-cyclic codes, quasi-cyclic codes.

1. Introducción

En la actualidad los anillos de Galois han adquirido notoriedad en las áreas de la teoría de códigos (cf. [1], [8], [11], [15], [18]) y la criptografía (cf. [3], [14]), entre otras. La teoría de códigos y la criptografía inmersas en las Matemáticas y en otras disciplinas tales como las ciencias de la computación e ingeniería eléctrica, están enfocadas en la optimización de la fiabilidad y seguridad de las comunicaciones digitales. A grandes rasgos, la fiabilidad significa corrección de errores mientras que la seguridad significa prevenir el acceso no autorizado de intrusos.

La teoría de códigos algebraicos sobre anillos finitos conmutativos con identidad adquirió relevancia con los trabajos de Nechaev [13] y Hammons et. al., [7]. Los anillos de Galois, al pertencer a esta familia de anillos, también han tenido una participación activa en el desarrollo de esta teoría (cf. [8], [11], [12] y [18]).

En el presente artículo estudiamos una forma de operar las μ-reducciones de las componentes p-ádicas de los elementos del anillo de Galois $\mathcal{R} = GR(p^3, m)$ y un isomorfismo entre éste y el anillo truncado de vectores de Witt de longitud 3, $W_3(\mathbb{F}_{p^m})$, para posteriormente a través de la isometría de Gray, dar condiciones necesarias y suficientes para que la imagen bajo la función de Gray de un $\mathcal{R}$-código *consta-cíclico* sea un $\mathbb{F}_{p^m}$-código *cuasi-cíclico*.

En la Sección 2 revisamos los anillos de Galois (cf. [17]), el enfoque está centrado principalmente en las propiedades básicas y una caracterización de los mismos. En la Sección 3, examinamos el formalismo de la construcción del anillo de vectores de Witt, para tal propósito nos basamos en [6] y [9]. Después, en la Sección 4, comentamos el isomorfismo entre los anillos de Galois de índice de nilpotencia n y el anillo truncado de vectores de Witt de longitud n dado en [16]. Posteriormente, en la Sección 5, se presentarán fórmulas para las μ-reducciones de las componentes p-ádicas de la adición en $\mathcal{R}$ y el producto de un elemento arbitrario de $\mathcal{R}$ con una unidad de la forma $\lambda = 1 - p^2$. Finalmente, en la Sección 6, establecemos condiciones necesarias y suficientes para que la imagen bajo la función de Gray de un $\mathcal{R}$-código consta-cíclico sea cuasi-cíclica sobre $\mathbb{F}_{p^m}$.

2. Anillos de Galois

Los anillos de Galois son extensiones únicas del anillo de clases residuales $\mathbb{Z}_{p^s} = \mathbb{Z}/p^s\mathbb{Z}$ con s un entero positivo y p un número primo. Estos anillos (en particular $\mathbb{Z}_4$) resultaron de

importancia en los años 90, en el estudio de la caracterización de la estructura algebraica de los códigos cíclicos lineales sobre $\mathbb{Z}_4$. En [7] Hammons et. al., demostraron que el código de Kerdock, es la imagen de Gray de un código cíclico lineal extendido sobre $\mathbb{Z}_4$ (un análogo en $\mathbb{Z}_4$ de los códigos de Reed-Muller de primer orden); más aún, se demostró que los códigos de Preparata son a su vez análogos en $\mathbb{Z}_4$ a los códigos extendidos de Hamming. A partir de estos trabajos, los anillos finitos de cadena (a los cuales pertenecen los anillos de Galois) cobraron importancia en la teoría de códigos algebraicos (cf. [2], [4]).

Una particularidad que acompaña a los anillos de Galois (y que les da su nombre) son las múltiples similitudes con los campos finitos (cf. [10]). A continuación revisaremos los conceptos y propiedades principales de estos anillos.

Sean s un entero positivo y p un número primo. Denotamos por $\mathbb{Z}_{p^s} = \mathbb{Z}/p^s\mathbb{Z}$ el anillo de clases residuales módulo p^s, $\mathbb{Z}_{p^s}[x]$ el anillo de polinomios en la indeterminada x con coeficientes en $\mathbb{Z}_{p^s}$ y denotamos al ideal principal $\langle p1\rangle$ mediante (p). Definimos las funciones:

$$\begin{aligned} \mu : \mathbb{Z}_{p^s} &\to \tfrac{\mathbb{Z}_{p^s}}{(p)} \\ a &\mapsto a + (p) \end{aligned} \qquad\qquad \begin{aligned} \hat{\mu} : \mathbb{Z}_{p^s}[x] &\to \tfrac{\mathbb{Z}_{p^s}}{(p)}[x] \\ f(x) = \sum_{i=0}^{n} a_i x^i &\mapsto \hat{\mu}(f(x)) = \sum_{i=0}^{n} \mu(a_i) x^i. \end{aligned}$$

Se tiene que $\mu, \hat{\mu}$ son homomorfismos sobreyectivos llamados *μ-reducción* y *$\hat{\mu}$-reducción* respectivamente. Puede apreciarse que $\hat{\mu}$ es una extensión natural de μ sobre el anillo de polinomios $\mathbb{Z}_{p^s}[x]$. Un polinomio mónico $f(x) \in \mathbb{Z}_{p^s}[x]$ será llamado *básico irreducible* (*resp. básico primitivo*) si $\hat{\mu}(f(x)) \in \mathbb{F}_p[x]$ es irreducible (resp. primitivo).

Definición 2.1. Sea p un número primo. Un anillo finito $\mathcal{R}$, conmutativo con identidad 1, es un *anillo de Galois*, si el conjunto de sus divisores de cero $\mathcal{D}$, con el cero añadido, forman un ideal principal generado por 0 o por $p1$.

Ejemplo 2.2. Algunos ejemplos de anillos de Galois son:

1. Los campos finitos pues $\mathcal{D} = \emptyset$, así $\mathcal{D} \cup \{0\} = (0)$.
2. El anillo de clases residuales $\mathbb{Z}_{p^s}$ con $\mathcal{D} \cup \{0\} = (p)$.

Sea $\mathcal{R}$ un anillo de Galois, entonces contiene un subanillo isomorfo a $\mathbb{Z}_{p^s}$ el cual denotaremos por $Z_{p^s} = \{n1 : n \in \mathbb{Z}\}$ y todos sus ideales son de la forma $\left(p^k\right)$ con $k \in \{0, 1, \ldots, s\}$, formando la cadena:

$$(0) = (p^s) \subsetneq (p^{s-1}) \subsetneq \cdots \subsetneq (p) \subsetneq (p^0) = (1) = \mathcal{R}.$$

Obsérvese que el ideal principal (p) es el único ideal maximal de $\mathcal{R}$, es decir, $\mathcal{R}$ es un *anillo local* y su *campo residual* $RF = \mathcal{R}/(p)$ es isomorfo a $\mathbb{F}_{p^m}$ para algún entero positivo m. Un teorema de caracterización para los anillos de Galois es el siguiente:

Teorema 2.3. *Dados enteros positivos p, m, s con p un número primo, existe un polinomio básico primitivo $h(x)$ en $\mathbb{Z}_{p^s}[x]$ de grado m y:*

$$\mathcal{R} = GR(p^s, m) \simeq \frac{\mathbb{Z}_{p^s}[x]}{(h(x))}.$$

Las unidades del anillo $\mathcal{R}$ forman un grupo multiplicativo en el cual existe un elemento[1] ξ de orden $p^m - 1$ y que es raíz del polinomio $h(x)$. El conjunto $\mathcal{T} = \left\{0, 1, \xi, \ldots, \xi^{p^m-2}\right\}$ es llamado *conjunto de Teichmuller* y está constituido por representantes del campo residual RF en el anillo de Galois. En [17] se demuestra que cada elemento $c \in \mathcal{R}$ tiene una única *representación p-ádica* dada por:

$$c = \rho_0(c) + p\rho_1(c) + \cdots + p^{s-1}\rho_{s-1}(c), \tag{1}$$

donde $\rho_i(c) \in \mathcal{T}$ con $0 \leq i \leq s-1$. También, cada elemento de $\mathcal{R}$, posee una única representación de la forma:

$$c = c_0 + c_1\xi + c_2\xi^2 + \cdots + c_{m-1}\xi^{m-1}, \tag{2}$$

con $c_i \in \mathbb{Z}_{p^s}$ para $0 \leq i \leq m-1$, llamada *representación aditiva*. Dicha representación es de suma utilidad cuando se desea trabajar con morfismos sobre el anillo de Galois $\mathcal{R}$ en particular resulta conveniente para definir el *automorfismo generalizado de Frobenius*: $\Theta : \mathcal{R} \to \mathcal{R}$ el cual es un automorfismo que fija a los elementos del subanillo Z_{p^s} en $\mathcal{R}$ y está dado por:

$$\Theta\left(c_0 + c_1\xi + c_2\xi^2 + \cdots + c_{m-1}\xi^{m-1}\right) = c_0 + c_1\xi^{p^m} + c_2\xi^{2p^m} + \cdots + c_{m-1}\xi^{(m-1)p^m}. \tag{3}$$

Éste es un análogo al *automorfismo de Frobenius* en campos finitos:

$$\begin{aligned} \sigma : \mathbb{F}_q &\to \mathbb{F}_q \\ \alpha &\mapsto \alpha^q, \end{aligned} \tag{4}$$

el cual fija a los elementos del *subcampo primo* de $\mathbb{F}_q$ (cf. [10]). A su vez, Θ genera un grupo cíclico con la composición de funciones llamado *grupo de Galois* de $\mathcal{R}$ sobre $\mathbb{Z}_{p^s}$, denotado por $Gal\left(\mathcal{R}/\mathbb{Z}_{p^s}\right)$. Cuando consideramos a los elementos de $\mathcal{R}$ como en (2) denotamos $\mathcal{R} = \mathbb{Z}_{p^s}[\xi]$.

El lector puede ampliar su visión de los anillos de Galois y sus importantes conexiones con los campos finitos haciendo una lectura de [17].

3. Anillo de vectores de Witt

Existen diversas variantes de la construcción del anillo de vectores de Witt. Ernst Witt introdujo el concepto de los vectores que llevan su nombre en 1936 mientras estudiaba las extensiones p-abelianas a través de los trabajos de los precursores A. A. Albert, Artin-Schreier y Kummer. En este apartado seguiremos la construcción de estos vectores y su correspondiente anillo como se hace en [6] y [9].

[1] Dicho elemento es llamado *primitivo* en paralelismo con los campos finitos (cf. [16]).

Sean $\mathcal{Q} = \mathbb{Q}[x_i, y_j, z_k]$ el anillo de polinomios en las $3n$ indeterminadas x_i, y_j, z_k para $1 \leq i, j, k \leq n$, $\mathbb{N} = \{0, 1, 2, \ldots\}$ y $\mathcal{Q}^{\mathbb{N}}$ el anillo de las sucesiones infinitas de elementos de $\mathcal{Q}$, $a = (a_\nu)$ para $\nu \geq 0$. De manera similar, $\mathbb{Z}[x_i, y_j]$ representa el subanillo de $\mathcal{Q}$ formado por los polinomios en las $2n$ indeterminadas x_i, y_j donde $1 \leq i, j \leq n$. Note que $\mathcal{Q}^{\mathbb{N}}$ tiene las operaciones de suma y producto componente a componente, y los elementos $(0) = (0, 0, \ldots, 0, \ldots)$, $(1) = (1, 1, \ldots, 1 \ldots)$, son los neutros de las operaciones suma y producto, respectivamente.

Dados $a = (a_0, a_1, \ldots, a_{\nu-1}, a_\nu, \ldots) \in \mathcal{Q}^{\mathbb{N}}$ una sucesión y p un número primo, denotaremos mediante $P(a)$ a la sucesión:

$$(a_0^p, a_1^p, \ldots, a_{\nu-1}^p, \ldots),$$

y para cada $\nu \in \mathbb{N}$ definimos la siguiente relación de recurrencia:

$$a^{(0)} = a_0 \quad \text{y} \quad a^{(\nu+1)} = \left(P(a)\right)^{(\nu)} + p^{\nu+1} a_{\nu+1}. \tag{5}$$

Desarrollando (5) para los primeros valores de $\nu \geq 1$ tenemos:

$$\begin{aligned}
a^{(1)} &= a_0^p + pa_1 \\
a^{(2)} &= a_0^{p^2} + pa_1^p + p^2 a_2 \\
\vdots \quad &\vdots \qquad\quad \vdots \\
a^{(\nu)} &= a_0^{p^\nu} + pa_1^{p^{\nu-1}} + \cdots + p^{\nu-1} a_{\nu-1}^p + p^\nu a_\nu.
\end{aligned}$$

A continuación dotaremos a $\mathcal{Q}^{\mathbb{N}}$ con nuevas operaciones de suma y producto, para esto es necesario introducir dos funciones:

Definición 3.1. Sean $a, b \in \mathcal{Q}^{\mathbb{N}}$. Definimos las siguientes funciones:

$$\begin{aligned}
\phi : \mathcal{Q}^{\mathbb{N}} &\to \mathcal{Q}^{\mathbb{N}} \\
a &\mapsto \phi(a) := (a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots), \\
\psi : \mathcal{Q}^{\mathbb{N}} &\to \mathcal{Q}^{\mathbb{N}} \\
b &\mapsto \psi(b) := (c_0, c_1, \ldots, c_{n-1}, \ldots),
\end{aligned}$$

donde:

$$\begin{aligned}
c_0 &= b_0, \\
c_1 &= \frac{1}{p}\left(b_1 - c_0^p\right), \\
c_2 &= \frac{1}{p^2}\left(b_2 - c_0^{p^2} - pc_1^p\right), \\
&\vdots \\
c_{\nu-1} &= \frac{1}{p^{\nu-1}}\left(b_{\nu-1} - c_0^{p^{\nu-1}} - pc_1^{p^{\nu-2}} - \cdots - p^{\nu-2} c_{\nu-2}^p\right).
\end{aligned} \tag{6}$$

Existe una relación importante entre las funciones ϕ y ψ la cual se presenta a continuación:

Lema 3.2. *La función ϕ es una biyección y $\phi^{-1} = \psi$.*

Demostración. Sea $a = (a_0, a_1, \ldots, a_{n-1}, \ldots) \in \mathcal{Q}^{\mathbb{N}}$, entonces:

$$\begin{aligned}\psi\phi(a) &= \psi(a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots)\\ &= \psi(a_0, a_0^p + pa_1, \ldots, a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-2}a_{n-2}^p + p^{n-1}a_{n-1}, \ldots)\\ &= (c_0, c_1, \ldots, c_{n-1}, \ldots).\end{aligned}$$

Demostraremos por inducción el resultado. Para ver que $c_i = a_i$ para $i \in \{0, 1, \ldots\}$, el caso $i = 0$ resulta trivial por (5). Supongamos que para cada $i < n-1$, $c_i = a_i$, así por (6):

$$\begin{aligned}c_{n-1} &= \frac{1}{p^{n-1}}\Big(a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-2}a_{n-2}^p + p^{n-1}a_{n-1} - c_0^{p^{n-1}}\\ &\qquad - pc_1^{p^{n-2}} - \cdots - p^{n-2}c_{n-2}^p\Big)\\ &= \frac{1}{p^{n-1}}\Big(a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-2}a_{n-2}^p + p^{n-1}a_{n-1} - a_0^{p^{n-1}}\\ &\qquad - pa_1^{p^{n-2}} - \cdots - p^{n-2}a_{n-2}^p\Big)\\ &= \frac{1}{p^{n-1}}\left(p^{n-1}a_{n-1}\right) = a_{n-1},\end{aligned}$$

de ahí que:

$$\psi\phi(a) = (c_0, c_1, \ldots, c_{n-1}, \ldots) = a$$

Por otro lado, si $b = (b_0, b_1, \ldots, b_{n-1}, \ldots)$, entonces:

$$\phi\psi\left(b\right) = \phi\left(c_0, c_1, \ldots, c_{n-1}\ldots\right) = \left(c^{(0)}, c^{(1)}, \ldots, c^{(n-1)}\right).$$

Veamos que $c^{(i)} = b_i$ para cada $i \in \{0, 1, \ldots\}$, por (5) se tiene que $c_0 = b_0$. Supongamos que para $i < n-1$, $c^{(i)} = b_i$, sustituyendo c_{n-1} según (5) tenemos:

$$\begin{aligned}c^{(n-1)} &= c_0^{p^{n-1}} + pc_1^{p^{n-2}} + \cdots + p^{n-2}c_{n-2}^p\\ &\quad + p^{n-1}\left(\tfrac{1}{p^{n-1}}\left(b_{n-1} - c_0^{p^{n-1}} - pc_1^{p^{n-2}} - \cdots - p^{n-2}c_{n-2}^p\right)\right)\\ &= c_0^{p^{n-1}} + pc_1^{p^{n-2}} + \cdots + p^{n-2}c_{n-2}^p + b_{n-1} - c_0^{p^{n-1}} - pc_1^{p^{n-2}} - \cdots - p^{n-2}c_{n-2}^p\\ &= b_{n-1}.\end{aligned}$$

Así,

$$\psi\phi(b) = (b_0, b_1, \ldots, b_{n-1}, \ldots) = b. \qquad \boxtimes$$

La función ϕ resulta de gran utilidad para nuestro objetivo. Ahora podemos definir las nuevas operaciones en $\mathcal{Q}$ como sigue:

$$\begin{aligned}a \oplus b &:= \psi\left(\phi(a) + \phi(b)\right), \quad \text{y}\\ a \odot b &:= \psi\left(\phi(a)\phi(b)\right)\end{aligned} \tag{7}$$

Como consecuencias del Lema 3.2 tenemos las relaciones:

$$\phi(a \oplus b) = \phi(a) + \phi(b), \quad \text{y} \tag{8}$$
$$\phi(a \odot b) = \phi(a)\phi(b) \tag{9}$$

Ahora, de la definición de ϕ, si $c = a \oplus b$ y $d = a \odot b$, entonces:

$$(c^{(0)}, c^{(1)}, \ldots, c^{(n-1)}, \ldots) = (a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots) + (b^{(0)}, b^{(1)}, \ldots, b^{(n-1)}, \ldots),$$
$$(d^{(0)}, d^{(1)}, \ldots, d^{(n-1)}, \ldots) = (a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots) \cdot (b^{(0)}, b^{(1)}, \ldots, b^{(n-1)}, \ldots),$$

por consiguiente, para cada $\nu \geq 0$:

$$\begin{aligned} (a \oplus b)^{(\nu)} &= a^{(\nu)} + b^{(\nu)}, \quad \text{y} \\ (a \odot b)^{(\nu)} &= a^{(\nu)} b^{(\nu)}. \end{aligned} \tag{10}$$

Observese que de (5), cada $a^{(\nu)}$ es una expresión polinomial con coeficientes racionales en las componentes $a_0, a_1, \ldots, a_\nu$, omitiendo todas aquellas cuyo subíndice es mayor que ν. De manera análoga, para las expresiones en (10) existe, a su vez, para cada una de éstas una expresión polinomial con coeficientes racionales en a_i, b_j con $i, j \in \{0, 1, \ldots \nu\}$ que las representa.

Definición 3.3. El anillo $W(\mathcal{Q}) = (\mathcal{Q}^{\mathbb{N}}, \oplus, \odot)$ es llamado, **anillo de vectores de Witt**.

Proposición 3.4. *$W(\mathcal{Q})$ es un anillo conmutativo con identidad.*

Demostración. Resulta claro que las operaciones son cerradas, veamos que los elementos neutros de las operaciones definidas en (7) son $(0, 0, \ldots, 0, \ldots)$ y $(1, 0, \ldots, 0, \ldots)$ respectivamente. Sea $a = (a_0, a_1, \ldots, a_{n-1}, \ldots)$, entonces:

$$\begin{aligned} (a_0, a_1, \ldots, a_{n-1}, \ldots) \oplus (0, 0, \ldots, 0, \ldots) &= \psi(\phi((a_0, a_1, \ldots, a_{n-1}, \ldots)) + \\ &\quad \phi((0, 0, \ldots, 0, \ldots))) \\ &= \psi((a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots) + \\ &\quad (0^{(0)}, 0^{(1)}, \ldots, 0^{(n-1)}, \ldots)) \\ &= \psi((a^{(0)} + 0^{(0)}, a^{(1)} + 0^{(1)}, \ldots, \\ &\quad \ldots, a^{(n-1)} + 0^{(n-1)}, \ldots)) \\ &= \psi((a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots)) \\ &= \psi(\phi((a_0, a_1, \ldots, a_{n-1}, \ldots))) \\ &= (a_0, a_1, \ldots, a_{n-1}, \ldots). \end{aligned}$$

Como $\phi((1,0,\ldots,0,\ldots)) = (1,1,\ldots,1,\ldots)$, tenemos que:

$$\begin{aligned}(a_0,a_1,\ldots,a_{n-1},\ldots)\odot(1,0,\ldots,0,\ldots) &= \psi(\phi((a_0,a_1,\ldots,a_{n-1},\ldots))\cdot\\ &\qquad \phi((1,0,\ldots,0,\ldots)))\\ &= \psi((a^{(0)},a^{(1)},\ldots,a^{(n-1)},\ldots)\cdot\\ &\qquad (1,1,\ldots,1,\ldots))\\ &= \psi((a^{(0)},a^{(1)},\ldots,a^{(n-1)},\ldots)\\ &= \psi(\phi((a_0,a_1,\ldots,a_{n-1},\ldots)))\\ &= (a_0,a_1,\ldots,a_{n-1},\ldots)\,.\end{aligned}$$

El resto de las propiedades de anillo pueden demostrarse usando las ecuaciones (8), (9) y (10). Por ejemplo:

$$\begin{aligned}\phi((a\oplus b)\odot c) &= \phi((a\oplus b))\phi(c)\\ &= \phi\left(\psi\left(\phi(a)+\phi(b)\right)\right)\phi(c)\\ &= \left(\phi(a)+\phi(b)\right)\phi(c)\\ &= \phi(a)\phi(c)+\phi(b)\phi(c)\\ &= \phi\left(\psi\left(\phi(a)\phi(c)\right)\right)+\phi\left(\psi\left(\phi(b)\phi(c)\right)\right)\\ &= \phi(a\odot c)+\phi(b\odot c),\end{aligned}$$

y así por el Lema 3.2, $(a\oplus b)\odot c = (a\odot c)\oplus(b\odot c)$. ☑

En lo sucesivo, denotaremos a los neutros de $\oplus$ y $\odot$ mediante $\mathbf{0}$ y $\mathbf{1}$, respectivamente.

Ahora, presentaremos algunos resultados que nos serán de ayuda en la construcción del anillo de vectores de Witt sobre anillos más generales.

Lema 3.5. *Sean $m\geq 1$, $0\leq i,j,k\leq m-1$, $a=(a_\nu), b=(b_\nu)$ elementos de $\mathcal{Q}^{\mathbb{N}}$ tales que $a_\nu, b_\nu\in\mathbb{Z}[x_i,y_j]$ con $0\leq\nu\leq m-1$. Entonces:*

$$a_\nu \equiv b_\nu \pmod{p^m} \qquad (0\leq\nu\leq k)$$

si, y solo si;

$$a^{(\nu)} \equiv b^{(\nu)} \pmod{p^{m+\nu}} \qquad (0\leq\nu\leq k).$$

Demostración. (cf.[6, Lemma 1]) ☑

Lema 3.6. *Sean $\varphi(x) = c_0+c_1x+\ldots+c_rx^r\in\mathbb{Z}[x]$, $r\in\mathbb{N}$ y p un número primo. Entonces $(\varphi(x))^p\equiv\tilde{\varphi}(x^p) \pmod{p}$ donde $\tilde{\varphi}(t)\in\mathbb{Z}[t]$.*

Demostración. Hagamos inducción en r. Para $r=1$ tenemos que $\varphi(x)=c_0+c_1x$. Es claro que:

$$(\varphi(x))^p = (c_0+c_1x)^p = c_0^p+\sum_{j=1}^{p-1}\tbinom{p}{j}(c_0)^{p-j}(c_1x)^j+c_1^px^p.$$

Luego, $(\varphi(x))^p - [c_0^p + c_1^p x^p] = \sum_{j=1}^{p-1} \binom{p}{j}(c_0)^{p-j}(c_1 x)^j$ y $p \mid \binom{p}{j}$ si $1 \leq j \leq p-1$. Note que si elegimos $\tilde{\varphi}(t) = c_0^p + c_1^p t$, entonces $(\varphi(x))^p \equiv \tilde{\varphi}(x^p) \pmod{p}$.

Supongamos que el grado de φ es menor que r, así, el resultado es válido y sea $\varphi(x) = c_0 + c_1 x + \ldots + c_r x^r$. Por lo tanto, $f(x) = \varphi(x) - c_r x^r \in \mathbb{Z}[x]$ es un polinomio de grado menor que r. De la hipótesis inductiva tenemos:

$$(f(x))^p \equiv \tilde{f}(x^p) \pmod{p},$$

donde $\tilde{f}(t) \in \mathbb{Z}[t]$. Más aún, como $(\varphi(x) - c_r x^r)^p = (f(x))^p$, entonces

$$(\varphi(x) - c_r x^r)^p \equiv \tilde{f}(x^p) \pmod{p}. \tag{11}$$

Por otro lado, es fácil ver que procediendo como antes, obtenemos que $(\varphi(x) - c_r x^r)^p \equiv (\varphi(x))^p - c_r^p x^{pr} \pmod{p}$. Luego, combinando esto con (11) concluimos

$$(\varphi(x))^p - c_r^p x^{pr} \equiv \tilde{f}(x^p) \pmod{p}.$$

Definamos $\tilde{\varphi}(t) = \tilde{f}(t) + c_r^p t^r$ y de lo anterior se sigue el resultado. ☑

Este resultado puede extenderse de manera natural por inducción a polinomios en múltiples variables $x_1, x_2, \ldots, x_k$ para k un entero positivo como sigue:

Corolario 3.7. *Sean $f(\underline{x}) \in \mathbb{Z}[\underline{x}]$ y p un número primo. Entonces $(f(\underline{x}))^p \equiv \tilde{f}(\underline{x}^p) \pmod{p}$ para algún $\tilde{f}(\underline{t}) \in \mathbb{Z}[\underline{t}]$, donde $f(\underline{x}) := f(x_1, x_2, \ldots, x_k)$, $\tilde{f}(\underline{x}^p) := \tilde{f}(x_1^p, x_2^p, \ldots, x_k^p)$ y $\mathbb{Z}[\underline{u}] := \mathbb{Z}[u_1, u_2, \ldots, u_k]$ para $u = x$ o $u = t$.*

Ahora, aplicando los resultados anteriores estableceremos una caracterización de las operaciones de dos elementos en $W(\mathcal{Q})$ bajo $\oplus$ y $\odot$, lo cual es de sumo interés para lograr nuestro objetivo.

Teorema 3.8. *Sean $a, b \in W(\mathcal{Q})$. Si $a \circ b$ representa $a \oplus b$ o $a \odot b$ y $a \hat{\circ} b$ representa $a + b$ ó $a \cdot b$, según sea el caso, entonces $(a \circ b)_\nu = f_\nu(a_i, b_j)$ donde $f_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ es un polinomio con coeficientes enteros y término constante 0 en las variables x_i, y_j con i, j corriendo en el conjunto $\{0, 1, \ldots, \nu\}$.*

Demostración. Sean $a, b \in W(\mathcal{Q})$, entonces $(a \circ b) = ((a \circ b)_0, \ldots, (a \circ b)_{\nu-1}, (a \circ b)_\nu, \ldots)$ y para cada $\nu \geq 0$; $(a \circ b)_\nu = f_\nu(a_i, b_j)$, para algún $f_\nu(x_i, y_j) \in \mathbb{Q}[x_i, y_j]$. Veamos mediante inducción sobre ν que $f_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$. Si $\nu = 0$, por (5) y (10), tenemos que $(a \circ b)_0 = (a \circ b)^{(0)} = a^{(0)} \hat{\circ}\, b^{(0)} = a_0 \hat{\circ} b_0 = f_0(a_0, b_0)$ donde $f_0(x_i, y_j) = 1x_i \hat{\circ}\, 1y_j \in \mathbb{Z}[x_i, y_j]$ y se sigue el resultado. Supongamos que $(a \circ b)_k = g_k(a_i, b_j)$ para algún $g_k(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ siempre que k es tal que $0 \leq k \leq \nu - 1$. Por (5) tenemos que:

$$p^\nu (a \circ b)_\nu = (a \circ b)^{(\nu)} - (P(a \circ b))^{(\nu-1)}, \tag{12}$$

y también:

$$(a \circ b)^{(\nu)} \equiv (P(a \circ b))^{(\nu-1)} \pmod{p^\nu}.$$

Por otro lado, $P((a \circ b)_k) = (a \circ b)_k^p = (g_k(a_i, b_j))^p$ y además, por el Corolario 3.7, existe $f_k(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ tal que:

$$P((a \circ b)_k) = (g_k(a_i, b_j))^p \equiv f_k(a_i^p, b_j^p) = f_k(P(a), P(b)) \pmod{p}.$$

Se sigue de lo anterior[2] que:

$$P((a \circ b)_k) \equiv (P(a) \circ P(b))_k \pmod{p} \quad (0 \leq k \leq \nu - 1).$$

En particular para $\nu - 1$, por el Lema 3.5:

$$(P(a \circ b))^{(\nu-1)} \equiv (P(a) \circ P(b))^{(\nu-1)} \pmod{p^\nu}.$$

Por (5) tenemos que $a^{(\nu)} \equiv (P(a))^{(\nu-1)} \pmod{p^\nu}$ y $b^{(\nu)} \equiv (P(b))^{(\nu-1)} \pmod{p^\nu}$, y por (10) se tiene que $(a \circ b)^{(\nu)} = a^{(\nu)} \hat{\circ} b^{(\nu)}$, por consiguiente:

$$(a \circ b)^{(\nu)} = a^{(\nu)} \hat{\circ}\, b^{(\nu)} \equiv (P(a))^{(\nu-1)} \hat{\circ}\, (P(b))^{(\nu-1)} \pmod{p^\nu},$$

y como $(P(a))^{(\nu-1)} \hat{\circ}\, (P(b))^{(\nu-1)} \equiv (P(a) \circ P(b))^{(\nu-1)} \pmod{p^\nu}$ tenemos que:

$$(a \circ b)^{(\nu)} \equiv (P(a) \circ P(b))^{(\nu-1)} \pmod{p^\nu}.$$

Se sigue que $p^\nu \mid [(a \circ b)^{(\nu)} - (P(a \circ b))^{(\nu-1)}]$, i.e., p^ν es un factor de la diferencia de las evaluaciones polinomiales que corresponden a $(a \circ b)^{(\nu)}$ y $(P(a \circ b))^{(\nu-1)}$. Por la hipótesis inductiva existe un polinomio $g_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ tal que:

$$g_\nu(a_i, b_j) = (a \circ b)^{(\nu)} - (P(a \circ b))^{(\nu-1)}$$

y por lo anterior $g_\nu(x_i, y_j) \in p^\nu \mathbb{Z}[x_i, y_j]$, de ahí que existe $f_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ tal que $g_\nu(x_i, y_j) = p^\nu f_\nu(x_i, y_j)$. Finalmente, de (12) tenemos que el polinomio $g_\nu(x_i, y_j)$ es tal que $p^\nu (a \circ b)_\nu = g_\nu(a_i, b_j) = p^\nu f_\nu(a_i, b_j)$ y dado que $f_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ esto concluye la demostración. ☑

En virtud del teorema anterior podemos denotar en lo sucesivo para $(a_\nu), (b_\nu) \in W(\mathcal{Q})$:

$$\begin{aligned} (a \oplus b)_\nu &= s_\nu(a_0, a_1, \ldots, a_{\nu-1}, b_0, b_1, \ldots, b_{\nu-1}) = s_\nu(a_i, b_j), \quad \text{y} \\ (a \odot b)_\nu &= m_\nu(a_0, a_1, \ldots, a_{\nu-1}, b_0, b_1, \ldots, b_{\nu-1}) = m_\nu(a_i, b_j), \end{aligned} \tag{13}$$

donde $s_\nu, m_\nu \in Z[x_i, y_j]$ para $\nu \geq 0$ y $0 \leq i, j \leq \nu$.

Sea A un anillo conmutativo con identidad 1_A de característica p, notemos que $\mathbb{Z}[x_i, y_j, z_k] \subseteq \mathbb{Q}[x_i, y_j, z_k]$ puede ser sumergido en el anillo de polinomios $A[X_i, Y_j, Z_k]$ mediante:

$$\begin{aligned} \lambda : \mathbb{Z}[x_i, y_j, z_k] &\to A[X_i, Y_j, Z_k] \\ n &\mapsto n1_A \qquad\qquad (n \in \mathbb{Z}) \\ x_i &\mapsto X_i \\ y_j &\mapsto Y_j \\ z_k &\mapsto Z_k. \end{aligned}$$

Dado $f(x_i, y_j, z_k) \in \mathbb{Z}[x_i, y_j, z_k]$ denotamos por $\hat{f}(X_i, Y_j, Z_k)$ a $\lambda(f(x_i, y_j, z_k))$. Por otro lado, a la luz del Teorema 3.8, las operaciones $\oplus$, $\odot$ son cerradas al tomar

[2]La expresión polinomial $f_k(P(a), P(b))$ sólo toma las primeras k componentes de $P(a)$ y $P(b)$.

$a, b \in \mathbb{Z}[x_i, y_j, z_k]^{\mathbb{N}}$ y $\mathbf{0}, \mathbf{1} \in \mathbb{Z}[x_i, y_j, z_k]^{\mathbb{N}}$, es decir, éste es un subanillo de $W(\mathcal{Q})$ que denotaremos por $W(\mathbb{Z})$. Ahora consideremos los conjuntos de sucesiones infinitas: $A^{\mathbb{N}}$ y $(\lambda(\mathbb{Z}[x_i, y_j, z_k]))^{\mathbb{N}}$, entonces $\lambda : \mathbb{Z}[x_i, y_j, z_k] \to \lambda(\mathbb{Z}[x_i, y_j, z_k])$, es un homomorfismo de anillos sobreyectivo y puede ser extendido de manera natural como sigue:

$$\begin{aligned} \Lambda : W(\mathbb{Z}) &\to \mathcal{A} = (\lambda(\mathbb{Z}[x_i, y_j, z_k]))^{\mathbb{N}} \\ (f_\nu(x_i, y_j, z_k)) &\mapsto (\hat{f}_\nu(X_i, Y_j, Z_k)). \end{aligned}$$

Nuevamente, por el Teorema 3.8 dadas dos sucesiones $a, b \in W(\mathbb{Z})$ existen polinomios con coeficientes enteros s_ν, m_ν que satisfacen (13), así tenemos la siguiente definición.

Definición 3.9. Dados dos elementos $r = (r_\nu), t = (t_\nu) \in \mathcal{A}$ definimos la suma y el producto de estos como las sucesiones $r \oplus t = ((r + t)_\nu)$ y $r \odot t = ((rt)_\nu)$ tales que:

$$\begin{aligned} (r + t)_\nu = \Lambda(s_\nu(x_i, y_j)) = \hat{s}_\nu(r_i, t_j), \quad \text{y} \\ (st)_\nu = \Lambda(m_\nu(x_i, y_j)) = \hat{m}_\nu(r_i, t_j). \end{aligned} \tag{14}$$

Veamos que en efecto mediante las operaciones definidas antes, se puede dotar de una estructura de anillo a $\mathcal{A}$:

Teorema 3.10. *El conjunto $\mathcal{A}$ es un anillo conmutativo con identidad $(1_A, 0_A, \ldots, 0_A, \ldots)$ y neutro de la suma $(0_A, 0_A, \ldots, 0_A, \ldots)$*

Demostración. Sean $X = (X_0, X_1, \ldots, X_{n-1}, \ldots)$, $Y = (Y_0, Y_1, \ldots, Y_{n-1}, \ldots)$ y $Z = (Z_0, Z_1, \ldots, Z_{n-1}, \ldots) \in \mathcal{A}$. Como Λ es sobreyectiva, existen $x = (x_0, x_1, \ldots, x_{n-1}, \ldots)$, $y = (y_0, y_1, \ldots, y_{n-1}, \ldots)$, $z = (z_1, z_2, \ldots, z_{n-1}, \ldots) \in \mathbb{Z}^{\mathbb{N}}$ tales que $\Lambda(x) = X$, $\Lambda(y) = Y$ y $\Lambda(z) = Z$. Luego, por (14):

$$\begin{aligned} (X + Y)_\nu = (\hat{s}_\nu(X_i, Y_j)) = \Lambda(s_\nu(x \oplus y)_\nu), \quad \text{y} \\ (XY)_\nu = (\hat{m}_\nu(x_i, y_j)) = \Lambda(m_\nu(x \odot y)_\nu), \end{aligned}$$

y esto se cumple para cada $\nu \geq 0$, entonces:

$$\begin{aligned} \Lambda(x) \oplus \Lambda(y) = X \oplus Y = \Lambda(x \oplus y), \quad \text{y} \\ \Lambda(x) \odot \Lambda(y) = X \odot Y = \Lambda(x \odot y), \end{aligned}$$

es decir, Λ preserva las operaciones entre $W(\mathbb{Z})$ y $\mathcal{A}$, en otras palabras, Λ es un homomorfismo sobreyectivo de anillos, así por el primer teorema de isomorfismos:

$$\mathcal{A} \simeq \frac{W(\mathbb{Z})}{\ker(\Lambda)}.$$

Finalmente, dado que $\Lambda(\mathbf{1}) = (1_A, 0_A, \ldots, 0_A, \ldots)$ y $\Lambda(\mathbf{0}) = (0_A, 0_A, \ldots, 0_A, \ldots)$, estos son la identidad y el neutro de la suma en $\mathcal{A}$ respectivamente. ☑

El teorema anterior establece un hecho importante, puesto que nos ha bastado con hallar una imagen homomórfica del anillo de polinomios en varias indeterminadas (x_i, y_j, z_k) con coeficientes en $\mathbb{Z}$ para poder extender la estructura del anillo de vectores de Witt

$W(\mathcal{Q})$ al conjunto de sucesiones infinitas $\mathcal{A}$. Esto resulta muy útil dado que si $A = \mathbb{F}_{p^m}$ las condiciones se satisfacen de manera inmediata y nos acerca a nuestro objetivo.

Es importante reconocer la diferencia al usar $\mathbb{Z}[x_i, y_j, z_k]^{\mathbb{N}}$ y $W(\mathbb{Z})$ pues el primero hace referencia a las sucesiones con las operaciones usuales de suma y producto, mientras que el segundo nos debe indicar que estamos usando la estructura inducida mediante $\oplus$ y $\odot$. El siguiente corolario es el paso final en la construcción del anillo truncado de vectores de Witt.

Corolario 3.11. *Sean*

$$W_{(s)}(A) = \{(r_\nu) \in W(A) : r_\nu = 0_A, \nu \geq s\},$$
$$W_s(A) = \{(r_0, r_1, \ldots, r_{s-1}) : r_i \in A, 0 \leq i \leq s-1\},$$

y la función:

$$\begin{aligned} \tau : W_{(s)}(A) &\to W_s(A) \\ (r_\nu) &\mapsto (r_0, r_1, \ldots, r_{s-1}). \end{aligned} \tag{15}$$

Si definimos la suma $+_s$ y el producto $\cdot_s$ en $W_s(A)$ mediante:

$$(r_0, r_1, \ldots, r_{s-1}) +_s (t_0, t_1, \ldots, t_{s-1}) = \tau(r \oplus t), \quad \text{y}$$
$$(r_0, r_1, \ldots, r_{s-1}) \cdot_s (t_0, t_1, \ldots, t_{s-1}) = \tau(r \odot t),$$

entonces $(W_s(A), +_s, \cdot_s)$ es un anillo conmutativo con identidad $1 = (1_A, 0_A, \ldots, 0_A)$ y neutro de la suma $0 = (0_A, 0_A, \ldots, 0_A)$.

Definición 3.12. Sea A un anillo conmutativo con identidad. Los anillos conmutativos $(W(A), \oplus, \odot)$ y $(W_s(A), +_s, \cdot_s)$ asociados a A, reciben los nombres de *anillo de vectores de Witt sobre el anillo A* y *anillo truncado de vectores de Witt de longitud s* sobre A, respectivamente.

En la sección 2 se mencionaron dos representaciones para elementos del anillo de Galois, la representación p-ádica (1) y la representación aditiva (2), la diferencia sustancial entre dichas formas de escribir los elementos del anillo estriba en que, mientras que las representaciónes aditivas son fáciles de operar mediante la suma y producto *usuales* en $\mathbb{Z}_{p^s}[\xi]$, las representaciones p-ádicas, por otro lado, representan un problema mayor, ya que sus *coeficientes* deben ser elementos del conjunto de Teichmüller $\mathcal{T}$ el cual en general no es cerrado bajo la suma, pero como la μ-reducción resulta ser una biyección entre $\mathcal{T}$ y $\mathbb{F}_{p^m}$, éste hecho permitirá posteriormente dar una solución a dicha problemática, más aún, en [16], los autores presentan un isomorfismo entre el anillo truncado de vectores de Witt $W_s(\mathbb{F}_{p^m})$ y el anillo de Galois $GR(p^s, m)$ luego, haciendo uso de esta herramienta se consigue operar a las μ-reducciones de las componentes p-ádicas de los elementos del anillo de Galois.

Dicho resultado se enuncia a continuación, en lo sucesivo, denotaremos mediante $\overline{\rho}_i(c)$ a $\mu(\rho_i(c))$ la μ-reducción de las componentes p-ádicas de un elemento $c \in GR(p^s, m)$.

Teorema 3.13 ([16, Theorem 4]). *El anillo truncado de vectores de Witt de longitud s, $W_s(\mathbb{F}_{p^m})$ es isomorfo al anillo de Galois $GR(p^s, m)$ mediante la función:*

$$\Gamma : GR(p^s, m) \to W_s(\mathbb{F}_{p^m})$$
$$c = \rho_0(c) + \rho_1(c)p + \cdots + \rho_{s-1}(c)p^{s-1} \mapsto \left(r_0(c), r_1(c)^p, \ldots, r_{s-1}(c)^{p^{s-1}}\right),$$

donde $\rho_i(c) \in \mathcal{T}$, $(0 \leq i \leq s-1)$ son las componentes p-ádicas del elemento $c \in GR(p^s, m)$ como en (1) *y $r_i(c) = \overline{\rho_i}(c)$.*

4. Aritmética en $GR(p^3, m)$

A continuación estudiaremos cómo el isomorfismo Γ del Teorema 3.13 nos permite estudiar la suma de dos elementos cualesquiera en el anillo $GR(p^3, m)$ y el producto de un elemento arbitrario en dicho anillo con una unidad de la forma $\lambda = 1 - p^2$.

Se conseguirán fórmulas para dichas operaciones y éstas nos permitirán estudiar también la aritmética de las componentes p-ádicas de los elementos en un anillo de Galois. Vale la pena remarcar la importancia de hallar una manera esquemática de operar dichas componentes y más adelante usaremos esto para analizar códigos definidos sobre $GR(p^3, m)$.

Consideremos el caso $s = 2$. Dados elementos $(u_0, u_1), (v_0, v_1) \in W_2(\mathbb{F}_{p^m})$, aplicando (15) a (10) tenemos que:

$$(s_0, s_1)^{(\nu)} = ((u_0, u_1) +_2 (v_0, v_1))^{(\nu)} = (u_0, u_1)^{(\nu)} + (v_0, v_1)^{(\nu)}.$$

Por (5) tenemos las siguientes expresiones:

$$\begin{aligned} s_0 &= u_0 + v_0, \quad \text{y} \\ s_0^p + ps_1 &= u_0^p + pu_1 + v_0^p + pv_1. \end{aligned} \tag{16}$$

Notemos que:

$$s_0^p = u_0^p + v_0^p + \sum_{i=1}^{p-1} \tbinom{p}{i} u_0^i v_0^{p-i}.$$

De (16) y lo anterior tenemos:

$$\begin{aligned} ps_1 &= (u_0^p + v_0^p - s_0^p) + p(u_1 + v_1), \\ ps_1 &= -\sum_{i=1}^{p-1} \tbinom{p}{i} u_0^i v_0^{p-i} + p(u_1 + v_1), \quad \text{y} \\ s_1 &= u_1 + v_1 + h_0(u_0, v_0), \end{aligned}$$

donde

$$h_0(u_0, v_0) = -\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} u_0^i v_0^{p-i}.$$

Para los términos s_ν con $\nu \geq 3$ la expresión es mucho más compleja, por lo tanto presentamos el siguiente resultado.

Lema 4.1. *Sean* $u = (u_0, u_1, \ldots, u_{s-1}), v = (v_0, v_1, \ldots, v_{s-1}) \in W_s(\mathbb{F}_{p^m})$. *Entonces:*

$$(u +_s v)_\nu = u_\nu + v_\nu - h_{\nu-1}(u_i, v_j), \tag{17}$$

donde $0 \leq i, j \leq \nu - 1$ *y* $h_l(x_i, y_j)$ *es un polinomio con coeficientes enteros y término constante (respecto a todas sus variables) cero, para* $0 \leq l \leq \nu - 1$ *y* $0 \leq \nu \leq s - 1$.

Demostración. Por (10) tenemos que $(u +_s v)^{(\nu)} = u^{(\nu)} + v^{(\nu)}$, ahora expandiendo como en (5) y si denotamos por s_k a $s_k(u_i, v_j)$ tenemos que:

$$\begin{aligned} s_0^{p^\nu} + ps_1^{p^{\nu-1}} + \cdots + p^{\nu-1}s_{\nu-1}^p + p^\nu s_\nu = &\left(u_0^{p^\nu} + pu_1^{\nu-1} + \cdots + p^{\nu-1}u_{\nu-1}^p + p^\nu u_\nu\right) \\ &+ \left(v_0^{p^\nu} + pv_1^{\nu-1} + \cdots + p^{\nu-1}v_{\nu-1}^p + p^\nu v_\nu\right). \end{aligned}$$

Despejando $p^\nu s_\nu$:

$$\begin{aligned} p^\nu s_\nu &= p^\nu(u_\nu + v_\nu) + \sum_{k=0}^{\nu-1} p^k \left(u_k^{p^{\nu-k}} + v_k^{p^{\nu-k}}\right) - \sum_{k=0}^{\nu-1} p^k s_k^{p^{\nu-k}} \\ &= p^\nu(u_\nu + v_\nu) + \sum_{k=0}^{\nu-1} p^k \left(u_k^{p^{\nu-k}} + v_k^{p^{\nu-k}} - s_k^{p^{\nu-k}}\right). \end{aligned} \tag{18}$$

Nombremos $h_{\nu-1}(u_i, v_j)$ al segundo término en el lado derecho de (18). Así, dividiendo por p^ν ambos lados de dicha ecuación, se obtiene (17). Las características de $h_l(x_i, y_j)$ se siguen del Teorema 3.8. ☑

Por otro lado, para la multiplicación sean $(u_0, u_1), (v_0, v_1) \in W_2(\mathbb{F}_{p^m})$. Procediendo como antes, tenemos:

$$\begin{aligned} m_0 &= u_0 v_0, \quad \text{y} \\ m_0^p + pm_1 &= (u_0^p + pu_1)(v_0^p + pv_1). \end{aligned}$$

Está claro que $m_0^p = u_0^p v_0^p$ y despejando m_1 tenemos que:

$$m_1 = u_0^p v_1 + v_0^p u_1 + p(u_1 v_1).$$

Reduciendo módulo p obtenemos $m_1 = u_0^p v_1 + v_0^p u_1$. Para poder hallar el nuevo término m_2 debemos tomar la expresión m_1 antes de la reducción módulo p, así:

$$\begin{aligned} m_1^p &= (u_0^p v_1 + v_0^p u_1 + p(u_1 v_1))^p \\ &= (u_0^p v_1 + v_0^p u_1)^p + \sum_{i=1}^{p-1} \tbinom{p}{i} (u_0^p v_1 + v_0^p u_1)^{p-i} p^i (u_1 v_1)^i + p^p u_1^p v_1^p \\ &= {u_0^p}^2 v_1^p + {v_0^p}^2 u_1^p + p\left[\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} (u_0^p v_1)^{p-i} (v_0^p u_1)^i\right] \\ &\quad + p^2\left[\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} (u_0^p v_1 + v_0^p u_1)^{p-i} p^{i-1} (u_1 v_1)^i + p^{p-2} u_1^p v_1^p\right]. \end{aligned} \tag{19}$$

De ahí, dado que $m_0^{p^2} = u_0^{p^2} v_0^{p^2}$ y

$$\begin{aligned} m_0^{p^2} + pm_1 + p^2 m_2 &= \left(u_0^{p^2} + pu_1^p + p^2 u_2\right)\left(v_0^{p^2} + pv_1^p + p^2 v_2\right) \\ &= u_0^{p^2} v_0^{p^2} + p\left[u_0^{p^2} v_1^p + v_0^{p^2} u_1^p\right] + p^2\left[u_0^{p^2} v_2 + u_1^p v_1^p + v_0^{p^2} u_2\right] + p^3\mathbf{T}, \end{aligned}$$

podemos agrupar términos semejantes y cancelar:

$$p^2 m_2 = p\left[u_0^{p^2} v_1^p + v_0^{p^2} u_1^p - m_1^p\right] + p^2\left[u_0^{p^2} v_2 + u_1^p v_1^p + v_0^{p^2} u_2\right] + p^3\mathbf{T}.$$

Aquí $\mathbf{T}$ representa a todos los términos que tienen como factor común a p^3; luego al dividir por p^2 quedará un factor p acompañando a $\mathbf{T}$, y estos términos desaparecerán al aplicar la reducción módulo p, por lo tanto, no es relevante (para este caso) conocerlos explícitamente. Usando (19) en la expresión anterior tenemos que:

$$p^2 m_2 = p^2\left[u_0^{p^2} v_2 + u_1^p v_1^p + v_0^{p^2} u_2 - \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} (u_0^p v_1)^{p-i} (v_0^p u_1)^i\right] + p^3\mathbf{T}'.$$

El último sumando de (19) está contenido en $\mathbf{T}'$ ahora debido al factor adicional p, y así tras dividir por p^2 y aplicar reducción módulo p:

$$m_2 = u_0^{p^2} v_2 + u_1^p v_1^p + v_0^{p^2} u_2 - \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} (u_0^p v_1)^{p-i} (v_0^p u_1)^i.$$

Es decir, que dados $(u_0, u_1, u_2), (v_0, v_1, v_2) \in W_3(\mathbb{F}_{p^m})$, entonces:

$$\begin{aligned} (u_0, u_1, u_2) +_3 (v_0, v_1, v_2) &= (u_0 + v_0, u_1 + v_1 + h_0(u_0, v_0), u_2 + v_2 + h_1(u_0, u_1, v_0, v_1)) \\ (u_0, u_1, u_2) \cdot_3 (v_0, v_1, v_2) &= \left(u_0 v_0, u_0^p v_1 + v_0^p u_1, u_0^{p^2} v_2 + u_1^p v_1^p + v_0^{p^2} u_2 - k(u_0, u_1, v_0, v_1)\right). \end{aligned} \tag{20}$$

Ahora podemos aplicar las fórmulas (20) para hallar las μ-reducciones de las componentes p-ádicas del producto de un elemento en el anillo de Galois $GR(p^3, m)$ y una unidad de la forma $\lambda = 1 - p^2$. Antes de hacerlo, un resultado que nos será de apoyo es la siguiente:

Proposición 4.2. *Sea $c \in R$. Entonces:*

$$r_j(p^k c) = \begin{cases} r_{k-j}(c), & k \le j \le 2; \\ 0 & \textit{de otro modo.} \end{cases}$$

para $0 \le k \le 2$.

Demostración. Sea $c \in R$ con representación p-ádica $c = \rho_0(c) + p\rho_1(c) + p^2\rho_2(c)$, entonces:

$$\begin{aligned} p^k c &= p^k\left(\rho_0(c) + p\rho_1(c) + p^2\rho_2(c)\right) \\ &= p^k\rho_0(c) + p^{k+1}\rho_1(c) + p^{k+2}\rho_2(c). \end{aligned}$$

Si $k = 1$, es claro que $pc = p\rho_0(c) + p^2\rho_1(c)$. Y dado que $\rho_0(c), \rho_1(c) \in \mathcal{T}$, se sigue de la unicidad de la representación p-ádica que:

$$\rho_0(pc) = 0, \rho_1(pc) = \rho_0(c) \text{ y } \rho_2(pc) = \rho_1(c). \tag{21}$$

Por otro lado, si $k = 2$, tenemos que $p^2c = p^2\rho_0(c)$. Y dado que $\rho_0(c) \in \mathcal{T}$, entonces:

$$\rho_0(p^2c) = \rho_1(p^2c) = 0 \text{ y } \rho_2(p^2c) = \rho_0(c). \tag{22}$$

Finalmente, aplicando la μ-reducción a las expresiones (21) y (22) se tiene el resultado. ☑

Ahora, considere una unidad en $\mathcal{R}$ de la forma $\lambda = 1 - p^2$, aplicando el isomorfismo Γ tenemos:

$$\Gamma(\lambda) = (r_0(\lambda), r_1(\lambda)^p, r_2(\lambda)^{p^2}) = (1, 0, -1).$$

Así, dado $c \in GR(p^3, m)$ con

$$\Gamma(c) = \left(r_0(c), r_1(c)^p, r_2(c)^{p^2}\right),$$

si aplicamos (20) para el producto λc tenemos que:

$$\begin{aligned} r_0(\lambda c) &= r_0(c) \\ r_1(\lambda c)^p &= r_1(c)^p \\ r_2(\lambda c)^{p^2} &= r_2(c)^{p^2} - r_0(c)^{p^2} - k(1, 0, r_0(c), r_1(c)). \end{aligned} \tag{23}$$

Es fácil ver de lo anterior que $k(1, 0, r_0(c), r_1(c)) = 0$ y aplicando el inverso del automorfismo de Frobenius a (23) en el campo finito $\mathbb{F}_{p^m}$ se llega a:

$$\begin{aligned} r_0(\lambda c) &= r_0(c), \\ r_1(\lambda c) &= r_1(c), \quad \text{y} \\ r_2(\lambda c) &= r_2(c) - r_0(c). \end{aligned}$$

5. Imágenes de Gray de códigos consta-cíclicos

En esta sección exhibiremos condiciones necesarias y suficientes para que la imagen de Gray de un código λ-cíclico o consta-cíclico sobre $\mathcal{R} = GR(p^3, m)$ sea cuasi-cíclica sobre el campo finito $\mathbb{F}_q$ con $q = p^m$ elementos. En adelante, sea $\mathcal{T}$ es el conjunto de Teichmüller de $\mathcal{R}$, $q = p^m$ y n es un entero positivo tal que $(n, p) = 1$.

Definición 5.1. Sea $\lambda = 1 - p^2 = 1 + N'p^2$, con $N' \in \mathcal{T}$ tal que $\mu(N') = -1$. Un corrimiento λ-cíclico o consta-cíclico es una función:

$$\begin{aligned} \nu_\lambda : R^n &\to R^n \\ (c_0, \ldots, c_{n-2}, c_{n-1}) &\mapsto (\lambda c_{n-1}, c_0, \ldots, c_{n-2}). \end{aligned}$$

Un código C es llamado *consta-cíclico* o λ-*cíclico* si, y solo si, $\nu_\lambda(C) \subseteq C$.

Definición 5.2. Sea $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$. Un *corrimiento cíclico* es una función:

$$\begin{aligned} \overline{\sigma} : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ (c_0, \ldots, c_{n-2}, c_{n-1}) &\mapsto (c_{n-1}, c_0, \ldots, c_{n-2}). \end{aligned}$$

Dados enteros positivos s, t tales que $st = n$ se puede escribir:

$$\underline{c}^{[k]} = \left(c_{k1}, \ldots, c_{ki}, \ldots, c_{ks}\right),$$

y por tanto:

$$\underline{c} = \left(\underline{c}^{[1]}, \ldots, \underline{c}^{[i]}, \ldots, \underline{c}^{[t]}\right).$$

Un *corrimiento cuasi-cíclico* $\sigma^{\otimes t} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ es una función tal que:

$$\sigma^{\otimes t}(c) = \left(\overline{\sigma}\left(c^{[1]}\right), \overline{\sigma}\left(c^{[2]}\right), \ldots, \overline{\sigma}\left(c^{[t]}\right)\right).$$

Un código $\mathcal{C}$ se dirá *cuasi-cíclico* de índice t y longitud st, si $\sigma^{\otimes t}(\mathcal{C}) = \mathcal{C}$.

Sean ω una raíz primitiva de la unidad en $\mathbb{F}_q$ y $\beta := \{1, \omega, \ldots, \omega^{m-1}\}$ una base de $\mathbb{F}_q$ como $\mathbb{F}_p$-espacio vectorial. Puesto que hay una biyección entre $\mathbb{Z}_q$ y $\mathbb{F}_q$ dada por:

$$h = h_0 + h_1 p + h_2 p^2 + \cdots + h_{m-1} p^{m-1} \mapsto \omega_h = h_0 + h_1 \omega + h_2 \omega^2 + \cdots + h_{m-1} \omega^{m-1},$$

donde $0 \leq h_i \leq p-1$ para $i = 0, 1, \ldots, m-1$, los elementos del campo finito $\mathbb{F}_q$, con $q = p^m$ elementos, se tomarán en el orden siguiente:

$$\mathbb{F}_q = \{\omega_h \mid h = 0, 1, \ldots, p^m - 1\}.$$

Obsérvese que,

$$\begin{aligned} \omega_{ip} + k = \omega_{ip+k} \text{ para } 0 \leq k \leq p-1 \text{ y } 0 \leq i \leq p^m - 1, \quad \text{y} \\ \omega_{ip+j} + k = \omega_{ip+(j+k)_p} \text{ para } 1 \leq j \leq p-1, 0 \leq k \leq p-1 \text{ y } 0 \leq i \leq p^m - 1, \end{aligned}$$

donde $(*)_p$ denota la reducción módulo p.

Sea

$$\Omega_i = (\omega_{ip}, \ldots, \omega_{ip+k}, \ldots, \omega_{ip+(p-1)}),$$

para $i = 0, 1, \ldots, p^{m-1} - 1$ y $k = 0, 1, \ldots, p-1$. Entonces los elementos del campo finito $\mathbb{F}_q$ se pueden expresar y enumerar en la forma:

$$(\omega_0, \omega_1, \ldots \omega_{p^m - 1}) = (\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^{m-1}-1}).$$

Definimos:

$$\begin{aligned} u &= (\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^{m-1}-1}), \\ v &= (\underbrace{1, \ldots, 1, \ldots, 1}_{q-veces}), \\ c_0 &= u \otimes v, \\ c_1 &= v \otimes u, \\ c_2 &= v \otimes v. \end{aligned}$$

Aquí, $\otimes$ denota el producto de Kronecker expandido de izquierda a derecha.

Definición 5.3. Sean $\mathcal{R} = GR(p^3, m)$, n un entero positivo y $RF = \mathbb{F}_q$ con $q = p^m$ entonces la función de Gray está dada por:

$$\begin{aligned} \Phi : \mathcal{R}^n &\to \mathbb{F}_q^{nq^2} \\ \underline{c} &\mapsto r_0(\underline{c}) \otimes c_0 + r_1(\underline{c}) \otimes c_1 + r_2(\underline{c}) \otimes c_2. \end{aligned} \tag{24}$$

La función de Gray resulta ser de gran importancia pues funciona como un puente entre los códigos definidos sobre anillos finitos de cadena y los códigos definidos sobre campos finitos (cf.[7], [18], [11]). Una de las propiedades más conocidas y que resulta de gran importancia en la teoría de códigos es el siguiente (cf. [4],[5]):

Teorema 5.4 ([4, Theorem 1.1])**.** *La función de Gray* Φ *es una isometría inyectiva entre* $(\mathcal{R}^n, \mathbf{d}_{hom})$ *y* $(\mathbb{F}_q^{nq^2}, d_H)$.

Aquí, $d_H(*)$ es la distancia de Hamming y $\mathbf{d}_{hom}(*)$ es la *distancia homogénea*, las cuales se definen de la siguiente manera: $d_H(\underline{c}, \underline{d}) = w_H(\underline{c} - \underline{d})$ y $\mathbf{d}_{hom} = \sum_{i=0}^{n-1} w_{hom}(c_i - d_i)$ donde

$$w_H(\underline{c}) = \Big| \{ i | c_i \neq 0 \quad 0 \leq i \leq n-1 \} \Big|,$$

y

$$w_{hom}(x) = \begin{cases} p^{2m}, & x \in (p^2) \setminus \{0\}; \\ p^m(p^m - 1), & x \in R \setminus (p^2); \\ 0, & x = 0. \end{cases}$$

El peso de Hamming y el peso homogéneo respectivamente.

Proposición 5.5.

$$\Phi \circ \nu_\lambda = \sigma^{\otimes p^{2m-1}} \circ \Phi.$$

Demostración. Sea $A = (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathcal{R}^n$ y denotemos por $B = (b_0, b_1, \ldots, b_{n-1}) = \nu_\lambda(A)$, entonces:

$$\begin{aligned} b_0 &= \lambda a_{n-1} \\ b_j &= a_{j-1} \qquad (1 \leq j \leq n-1), \end{aligned}$$

así de (23) tenemos:

$$\begin{aligned} r_0(B) &= (r_0(a_{n-1}), r_0(a_0), \ldots, r_0(a_{n-2})), \\ r_1(B) &= (r_1(a_{n-1}), r_1(a_0), \ldots, r_1(a_{n-2})), \quad \text{y} \\ r_2(B) &= (r_2(a_{n-1}) - r_0(a_{n-1}), r_2(a_0), \ldots, r_2(a_{n-2})). \end{aligned}$$

Ahora por (24) el k-ésimo bloque de longitud nq de $\Phi(B)$ es:

$$\begin{aligned} \Phi(B)^{[k]} &= r_0(B) \otimes u + r_1(B) \otimes \langle \omega_k \rangle_{p^m} + r_2(B) \otimes v \\ &= r_0(B) \otimes (\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^m-1}) + r_1(B) \otimes (\langle \omega_k \rangle_p, \ldots, \langle \omega_k \rangle_p, \ldots, \langle \omega_k \rangle_p) + \\ &\quad r_2(B) \otimes (\langle 1 \rangle_p, \ldots, \langle 1 \rangle_p, \ldots, \langle 1 \rangle_p). \end{aligned}$$

Así podemos extraer el i-ésimo bloque de longitud np de $\Phi(B)$ y lo denotaremos por $\mathcal{B}_i$

$$\mathcal{B}_i = r_0(B) \otimes \Omega_i + r_1(B) \otimes \langle \omega_k \rangle_p + r_2(B) \otimes \langle 1 \rangle_p.$$

Procediendo como antes y expandiendo los productos tenemos que:

$$\begin{aligned}\mathcal{B}_i = &(r_0(a_{n-1}), r_0(a_0), \ldots, r_0(a_{n-2})) \otimes (\omega ip, \ldots, \omega_{ip+j}, \ldots, \omega_{ip+(p-1)}) \\ &+ (r_1(a_{n-1}), r_1(a_0), \ldots, r_1(a_{n-2})) \otimes (\omega_k, \ldots, \omega_k, \ldots, \omega_k) \\ &+ (r_2(a_{n-1}) - r_0(a_{n-1}), r_2(a_0), \ldots, r_2(a_{n-2})) \otimes (1, \ldots, 1, \ldots, 1).\end{aligned}$$

Tras realizar los productos, podemos estudiar el j-ésimo bloque de longitud n de $\mathcal{B}_i$ el cual denotaremos por $\mathcal{B}_{ij}$ es decir:

$$\begin{aligned}\mathcal{B}_{ij} = &(r_0(a_{n-1})\omega_{ip+j}, r_0(a_0)\omega_{ip+j}, \ldots, r_0(a_{n-2})\omega_{ip+j}) \\ &+ (r_1(a_{n-1})\omega_k, r_1(a_0)\omega_k, \ldots, r_1(a_{n-2})\omega_k) \\ &+ (r_2(a_{n-1}) - r_0(a_{n-1}), r_2(a_0), \ldots, r_2(a_{n-2})).\end{aligned}$$

Notemos que la primera componente de $\mathcal{B}_{ij}$ es:

$$\begin{aligned}(\mathcal{B}_{ij})_0 = &\quad r_0(a_{n-1})\omega_{ip+j} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) - r_0(a_{n-1}) \\ = &\quad r_0(a_{n-1})\left(\omega_{ip+j} + (p-1)\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ = &\quad r_0(a_{n-1})\left(\omega_{ip+(j+p-1)_p}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ = &\quad r_0(a_{n-1})\left(\omega_{ip+(j-1)}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}).\end{aligned}$$

Se sigue que:

$$(\mathcal{B}_{ij})_0 = \quad r_0(a_{n-1})\left(\omega_{ip+(j-1)}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}), \quad \text{y} \tag{25}$$

$$(\mathcal{B}_{ij})_k = \quad r_0(a_{k-1})\omega_{ip+j} + r_1(a_{k-1})\omega_k + r_2(a_{k-1}) \qquad (1 \leq k \leq n-1). \tag{26}$$

Por otro lado, aplicando la función de Gray al n-tuple A obtenemos:

$$\Phi(A) = r_0(A) \otimes c_0 + r_1(A) \otimes c_1 + r_2(A) \otimes c_2.$$

Procediendo como antes analizaremos el i-ésimo bloque de longitud np de $\Phi(A)$ así:

$$\mathcal{A}_i = r_0(A) \otimes \Omega_i + r_1(A) \otimes \langle \omega_k \rangle_p + r_2(A) \otimes \langle 1 \rangle_p.$$

Expandiendo los productos de Kronecker de $\mathcal{A}_i$, podemos escribir dicho bloque como un arreglo de tamaño $n \times p$, es decir:

$$\mathcal{A}_i = \begin{pmatrix} r_0(a_0)\omega_{ip} + r_1(a_0)\omega_k + r_2(a_0) & \cdots & r_0(a_{n-1})\omega_{ip} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ \vdots & \cdots & \vdots \\ r_0(a_0)\omega_{ip+j} + r_1(a_0)\omega_k + r_2(a_0) & \cdots & r_0(a_{n-1})\omega_{ip+j} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ \vdots & \cdots & \vdots \\ r_0(a_0)\omega_{ip+(p-1)} + r_1(a_0)\omega_k + r_2(a_0) & \cdots & r_0(a_{n-1})\omega_{ip+(p-1)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \end{pmatrix}.$$

Observemos que al aplicar el corrimiento cíclico $\overline{\sigma}$ en este bloque:

$$\overline{\sigma}(\mathcal{A}_i) = \begin{pmatrix} r_0(a_{n-1})\omega_{ip+(p-1)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) & \cdots & r_0(a_{n-2})\omega_{ip} + r_1(a_{n-2})\omega_k + r_2(a_{n-2}) \\ \vdots & \cdots & \vdots \\ r_0(a_{n-1})\omega_{ip+(j-1)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) & \cdots & r_0(a_{n-2})\omega_{ip+j} + r_1(a_{n-2})\omega_k + r_2(a_{n-2}) \\ \vdots & \cdots & \vdots \\ r_0(a_{n-1})\omega_{ip+(p-2)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) & \cdots & r_0(a_{n-2})\omega_{ip+(p-1)} + r_1(a_{n-2})\omega_k + r_2(a_{n-2}) \end{pmatrix}.$$

Denotemos por $\mathcal{A}^{ij}$ al j-ésimo bloque de longitud n del arreglo $\overline{\sigma}(\mathcal{A}_i)$, de ahí tenemos que la 0-ésima y la k-ésima entradas de este bloque son respectivamente:

$$(\mathcal{A}^{ij})_0 = r_0(a_{n-1})\left(\omega_{ip+(j-1)}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}), \quad \text{y} \tag{27}$$

$$(\mathcal{A}^{ij})_k = r_0(a_{k-1})\omega_{ip+j} + r_1(a_{k-1})\omega_k + r_2(a_{k-1}) \qquad (1 \leq k \leq n-1). \tag{28}$$

Una comparación por pares de (25) con (27) y (26) con (28) respectivamente, nos permite llegar a que para cada $k \in \{0, 1, \ldots, n-1\}$ los bloques de longitud n; $\mathcal{B}_{ij}$ y $\mathcal{A}^{ij}$ son iguales, de ahí que

$$\mathcal{B}_i = \overline{\sigma}(\mathcal{A}_i) \qquad (0 \leq i \leq p^{m-1} - 1),$$

y dado que

$$\begin{aligned}\Phi(\nu_\lambda(A)) = \Phi(B) &= \left(\mathcal{B}_0 \mid \cdots \mid \mathcal{B}_i \mid \cdots \mid \mathcal{B}_{p^{m-1}-1}\right) \\ &= \left(\overline{\sigma}(\mathcal{A}_0) \mid \cdots \mid \overline{\sigma}(\mathcal{A}_i) \mid \cdots \mid \overline{\sigma}(\mathcal{A}_{p^{m-1}-1})\right) \\ &= \sigma^{\otimes p^{2m-1}}(\Phi(A)),\end{aligned}$$

se sigue el enunciado de la proposición. ☑

Esta proposición nos permite enunciar el resultado principal de está sección:

Teorema 5.6. *Un $\mathcal{R}$-código $\mathcal{C}$ de longitud n es consta-cíclico si, y solo si, su imagen bajo la función de Gray $\Phi(\mathcal{C})$ es un código cuasi-cíclico sobre $\mathbb{F}_{p^m}$ de índice p^{2m-1} y longitud np^{2m}.*

Demostración. Sea $\mathcal{C}$ un $\mathcal{R}$-código tal que $\Phi(\mathcal{C})$ es un código cuasi-cíclico de índice p^{2m-1} y longitud np^{2m}, entonces por definición:

$$\Phi(\mathcal{C}) = \sigma^{\otimes p^{2m-1}}(\Phi(\mathcal{C})).$$

Luego usando la Proposición 5.5:

$$\Phi(\mathcal{C}) = \Phi(\nu_\lambda(\mathcal{C})),$$

y de la inyectividad de Φ:

$$\mathcal{C} = \nu_\lambda(\mathcal{C}).$$

El recíproco de esta afirmación se sigue de manera análoga. ☑

6. Conclusiones

Los anillos de Galois tienen una conexión estrecha con el anillo truncado de vectores de Witt como se mostró con el isomorfismo del Teorema 3.13. Dicha conexión nos permitió establecer el Teorema 5.6.

A lo largo de este manuscrito una técnica recurrente ha sido el uso de las propiedades de las operaciones del anillo de vectores de Witt para analizar una forma adecuada de

operar los elementos del anillos de Galois mediante su representación p-ádica. Esto indica que al hacer uso de estas estructuras algebraicas en conjunto nos abre las puertas para investigar los códigos definidos sobre los anillos de Galois de manera eficiente.

Agradecimientos: Nos gustaría agradecer a los árbitros por sus valiosos comentarios y sugerencias que contribuyeron significativamente a mejorar la calidad de nuestro manuscrito.

Referencias

[1] Dinh H.Q., Liu H., Liu X. and Sriboonchitta S., "On structure and distances of some classes of repeated-root constacyclic codes over Galois rings", *Finite Fields Appl.*, 43 (2017), 86-105. doi: 10.1016/j.ffa.2016.09.004

[2] Dinh H.Q. and López-Permouth S.R., "Cyclic and negacyclic codes over finite chain rings", *IEEE Trans. Inform. Theory*, 50 (2004), No. 8, 1728-1744. doi: 10.1109/TIT.2004.831789

[3] Gómez-Calderon J. and Mullen G.L., "Galois rings and algebraic cryptography", *Acta Arith.*, 59 (1991), No. 4, 317-328. doi: 10.4064/aa-59-4-317-328.

[4] Greferath M. and Schmidt S.E., "Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code", *IEEE Trans. Inform. Theory*, 45 (1999), No. 7, 2522-2524. doi:10.1109/18.796395

[5] Nechaev A.A. and Khonol'd T., "Fully weighted modules and representations of codes", *Probl. Inf. Transm.*, 35 (1999), No. 3, 205-223; translation from Probl. Peredachi Inf., 35 (1999), No. 3, 18-39. **MR**1730800

[6] Jacobson N., Basic Algebra II, Dover Publications, 2nd ed., 2009, New York.

[7] Hammons Jr. A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A. and Solé P., "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes", *IEEE Trans. Inform. Tehory*, 40 (1994), No. 2, 301-319. doi: 10.1109/18.312154

[8] Kanwar P. and López-Permouth S.R., "Cyclic Codes over the Integers Modulo p^m", *Finite Fields Appl.*, 3 (1997), No. 4, 334-352. doi:10.1006/ffta.1997.0189

[9] Karpilovsky G., *Topics in field theory*, North-Holland Publishing Co., vol. 155, Amsterdam, 1989.

[10] Lidl R. and Niederreiter H., *Finite fields*, Cambridge University Press, 2nd ed.,vol. 20, Cambridge, 1997.

[11] Ling S. and Blackford J.T., "$\mathbb{Z}_{p^k+1}$-Linear Codes", *IEEE Trans. Inform. Theory*, 48 (2002), No. 9, 2592-2605. doi: 10.1109/TIT.2002.801473

[12] López-Andrade C.A. and Tapia-Recillas H., "On the linearity and quasi-cyclicity of the gray image of codes over a Galois ring", *Amer. Math. Soc.,* 537 (2011), 255-268. doi: 10.1090/conm/537/10580

[13] Nechaev A.A., "Kerdock code in a cyclic form", *Discrete Math. Appl.*, 1 (1991), No. 4, 365-384. doi:10.1515/dma.1991.1.4.365

[14] Özbudak F. and Saygi Z., "Some constructions of systematic authentication codes using galois rings", *Des. Codes Cryptogr.*, 41 (2006), No. 3, 343-357. doi: 10.1007/s10623-006-9021-x

[15] Sobhani R. and Esmaeili M., "Cyclic and negacyclic codes over the Galois ring $GR(p^2, m)$", *Discrete Appl. Math.*, 157 (2009), No. 13, 2892-2903. doi: 10.1016/j.dam.2009.03.001

[16] Shanbhag A.G., Kumar P.V. and Helleseth T., "An upper bound for the extended Kloosterman sums over Galois rings", *Finite Fields Appl.*, 4 (1998), No. 3, 218-238. doi: 10.1006/ffta.1998.0211

[17] Wan Z.X., *Lectures on finite fields and Galois rings*, World Scientific Publishing Co., Inc., River Edge, NJ, 2003. doi: 10.1142/5350

[18] Wolfmann J., "Binary images of cyclic codes over $\mathbb{Z}_4$", *IEEE Trans. Inform. Theory*, 47 (2001), No. 5, 1773-1779. doi: 10.1109/18.930917